



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/715,597

11/19/2003

Talal G. Shamoon

7451.0011-02

6441

22852

7590

01/29/2007

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER  
LLP

901 NEW YORK AVENUE, NW  
WASHINGTON, DC 20001-4413

EXAMINER

SHAN, APRIL YING

ART UNIT

PAPER NUMBER

2135

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
--	-----------	---------------

3 MONTHS

01/29/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

# Office Action Summary

Application No.

10/715,597

Applicant(s)

SHAMOON ET AL.

Examiner

April Y. Shan

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☐ Responsive to communication(s) filed on 19 November 2003.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 8-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 8-21 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 19 November 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 5/05 and 12/05
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application
- ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. Claims 8-21 have been examined. Claims 1-7 and 22-26 are canceled.

#### ***Specification***

2. Examiner is aware of the amended specification dated on 19 November 2003.

The application is a divisional of U.S. Application No. 09/276,233, filed March 25, 1999, which is a continuation-in-part of U.S. Application No. 09/270,022, filed March 16, 1999 (abandoned), both of which are incorporated herein by reference.

#### ***Claim Rejections - 35 USC § 103***

3. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

4. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

5. Claims 8-19 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over NPL publication, "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video", by Spanos, et al., as published by the "Proceedings of the Fourth ACM International Conference on Computer Communications and Network," September 1995, (hereinafter Spanos '95), in view of the NPL publication, "Applied Cryptography", by Schneier, published by John Wiley and Sons, 1996 (hereinafter Schneier '96), in view of Aucsmith (U.S. Patent No. 5,915,018 and hereinafter Aucsmith) and in view of Huizer et al. (U.S. Patent No. 5,875,303 and hereinafter Huizer et al.)

Since the Spanos '95 NPL publication relies on the reader having detailed knowledge of the internals of the DES encryption algorithm, examiner uses Schneier '96 to explicate DES as referred to in Spanos '95 and also to disclose the key transfer limitations in the claims.

As per **claim 8**, Spanos '95 discloses a method of encrypting and decrypting MPEG video data on an MPEG player. Specifically, Spanos '96 discloses: a streaming media player (Spanos '95: section Titled, "4. Aegis Performance", Page 4, col. 2, lines 43-45) providing content protection and digital rights management (Spanos '95: Section Titled, "3. Aegis Overview", Page 3, col. 2, lines 15-43), including:

a port configured to receive a digital bit stream (Spanos '95: Section Titled, "4. Aegis Performance", Page 4, col. 2, lines 43-45. Please note MPEG players of necessity have an input to receive a digital bit stream) the digital bit stream including: content which is encrypted at least in part (Spanos '95: Section Titled, "3. Aegis Overview", Page 3, col. 2, lines 15-43. Please note the encryption of only the I-frames), at least two sub-streams which have been muxed together, at least one of the sub-streams including compressed information (Spanos '95: Section Titled, "3. Aegis Overview", Page 3, col. 2, lines 16-29 - MPEG reads on substreams and compressed information) a control arrangement (Spanos '95: Section Titled, "5.1 Simulation Model", Page 5, col. 1, lines 40-41 - Please note MPEG player encoders and decoders read on a control arrangement) including: means for opening secure containers and extracting cryptographic keys, and means for decrypting the encrypted portion of the content;

Additionally, Spanos '95 explicitly discloses the use of the DES algorithm to encrypt the bit stream (Spanos '95: Section Titled, "3. Aegis Overview", Page 4, col. 1, line 30 - col. 2, line 3). However, Spanos '95 does not explicitly describe the DES algorithm, Examiner provides Schneier '96 to describe how DES reads on the remainder of the claim limitations.

Schneier '96 discloses the DES algorithm. Specifically, Schneier '96 discloses: control information for controlling use of the content, including at least one key suitable for decryption of at least a portion of the content (Schneier '96: Section Titled, "12.2 Description of DES", Page 270, lines 5-13 - note description of the key);

the control arrangement includes means for decrypting the encrypted portion of the content (Schneier '96: Section Titled, "12.2 Description of DES", Subsection Titled, "Decryption DES", Page 277, lines 11-22).

Furthermore, Schneier '96 discloses key transfer. Specifically, Schneier '96 discloses:

The bit stream includes a secure container including the control information which includes the key (Schneier '96: Section Titled, "8.3 Transferring Keys", Page 176, lines 38-43. Please note that Schneier '96 discloses "key-encryption keys" to encrypt "data keys" that may be transferred over the communication channel);

The control arrangement includes means for opening secure containers and extracting cryptographic keys (Schneier '96: Section Titled, "8.3 Transferring Keys", Page 176, lines 38-43)

It would be obvious to a person having ordinary skill in the art at the time of the invention to apply the key transfer of Schneier '96 to the encrypted MPEG player of Spanos '95. The motivation to combine is suggested by Schneier '96 which discloses the desirability of not transmitting a data key in the clear over a communications line (Schneier '96: Section Titled, "8.3 Transferring Keys", Page 176, lines 34-37).

The combined teachings of Spanos '95 and Schneier '96 do not disclose expressly the control arrangement contains a rule or rule set associated with governance of at least one sub-stream or object.

Aucsmith disclosed the control arrangement contains a rule or rule set associated with governance of at least one sub-stream or object (e.g. col. 3, lines 22-28, col. 4, lines 26-30, col. 5, lines 26-33 and col. 6, lines 22-30).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate Aucsmith's a rule or rule set associated with governance of at least one sub-stream or object into the player of Spanos '95 - Schneier '96.

The motivation of doing so would have been to "describe what sort of video controller is allowed access to the content" and "protecting the analog video output signal", as taught by Aucsmith (col. 5, lines 32-33 and col. 6, lines 25-26)

The combined teachings of Spanos '95 - Schneier '96 - Aucsmith do not explicitly disclose: wherein the player further includes: a demux designed to separate and route the sub-streams; a decompression unit configured to decompress at least one of the sub-streams, the decompression unit and the demux being connected by a pathway for the transmission of information; and a rendering unit designed to process decompressed content information for rendering.

Huizer et al. discloses the Philips <sup>TM</sup> Cdi <sup>TM</sup> media streaming player. Specifically, Huizer et al. discloses: wherein the player further includes:

a demux designed to separate and route the sub-streams (Huizer et al. : Fig. 6, item 71 (demux); col. 6, lines 60-65); a decompression unit configured to decompress at least one of the sub-streams, the decompression unit and the demux being connected by a pathway for the transmission of information (Huizer et al. : Fig. 6, items 71 (demux) and 5 (decoder which in the context of CDi and MPEG read on a decompression unit)

Art Unit: 2135

connected by items 72, 73 and 74); a rendering unit designed to process decompressed content information for rendering (Huizer et al. : col. 6, lines 55-57 ). It would have been obvious to a person having ordinary skill in the art to apply the configuration of Huizer et al. to the MPEG player of Spanos '95 and Schneier '96 in combination. The motivation to combine to include a demultiplexer, a decompression unit, and a rendering unit as taught by Huizer et al. is on the basis that these parts are integral and necessary to a streaming media player such as the MPEG player of Spanos '95 and Schneier '96 in combination.

Additionally, the combined teachings of Spanos '95 - Schneier '96 - Aucsmith - Huizer et al. disclose and a stream controller operatively connected to the decompression unit (Huizer et al. : FIG. 6, item 75 with items 71, 72, 73, 74 and 5), the stream controller including decryption functionality configured to decrypt at least a portion of a sub-stream (Spanos '95: Section Titled, "3. Aegis Overview", Page 4, col. 1, line 30 - col. 2, line 3. Please note the DES is integrated into the media player) based on at least one key passed from the control arrangement (Schneier '96: Section Titled, "8.3 Transferring Keys", Page 176, lines 38-43) and pass the decrypted sub-stream to the decompression unit (Spanos '95: Section Titled, "3. Aegis Overview", Page 4, col. 1, line 30 - col. 2, line 3. Please note the DES is integrated into the media player).

As per **claim 9**, the combined teachings of Spanos '95 – Schneier '96 – Aucsmith - Huizer et al. discloses a player as applied above in claim 8. Aucsmith further discloses wherein the rule or rule set is delivered from an external source (e.g. col. 7, lines 23-34).



As per **claim 10**, the combined teachings of Spanos '95 – Schneier '96 – Aucsmith - Huzer et al. discloses a player as applied above in claim 9. Aucsmith further discloses wherein the rule or rule set is delivered as part of the digital bit stream (e.g. col. 3, lines 21-28).

As per **claim 11**, the combined teachings of Spanos '95 – Schneier '96 – Aucsmith - Huzer et al. discloses a player as applied above in claim 8. Aucsmith further discloses wherein the rule or rule set specifies conditions under which the governed sub-stream or object may be decrypted (e.g. col. 7, line 63- col. 8, line 6).

As per **claim 12**, the combined teachings of Spanos '95 – Schneier '96 – Aucsmith - Huzer et al. discloses a player as applied above in claim 8. Aucsmith further discloses wherein the rule or rule set governs at least one aspect of access to or use of the governed sub-stream or object (e.g. col. 4, lines 26-30).

As per **claim 13**, the combined teachings of Spanos '95 – Schneier '96 – Aucsmith - Huzer et al. discloses a player as applied above in claim 12. Aucsmith further discloses wherein the governed aspect includes making copies of the governed sub-stream or object (e.g. col. 6, lines 22-30).

As per **claims 14-16**, the combined teachings of Spanos '95 – Schneier '96 – Aucsmith - Huzer et al. discloses a player as applied above in claim 12. Aucsmith further discloses wherein the governed aspect includes transmitting the governed sub-stream or object through a digital output port (e.g. col. 6, lines 22-30), wherein the rule or rule set specifies that the governed sub-stream or object can be transferred to a second device, but rendering of the governed sub-stream or object must be disabled in the first device prior to or during the transfer (e.g. col. 6, lines 22-30, col. 7, lines 8-22) and wherein the second device includes rendering capability, lacks at least one feature present in the streaming media player, and is at least somewhat more portable than the streaming media player (e.g. abstract and col. 4, lines 37- 42).

As per **claims 17-19**, the combined teachings of Spanos '95 – Schneier '96 – Aucsmith - Huzer et al. discloses a player as applied above in claim 11. Aucsmith further discloses wherein the control arrangement contains at least two rules governing access to or use of the same governed sub-stream or object ("rule set" – e.g. col. 4, line 26 ), wherein a first of the two rules was supplied by a first entity, and the second of the two rules was supplied by a second entity and wherein the first rule controls at least one aspect of operation of the second rule (e.g. col. 6, lines 22-30 and col. 7, lines 23-34).

As per **claim 21**, the combined teachings of Spanos '95 – Schneier '96 – Aucsmith - Huzer et al. discloses a player as applied above in claim 12. Aucsmith

further discloses wherein the governed aspect includes a requirement that audit information be provided (e.g. col. 6, lines 22-30).

6. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spanos '95 – Schneier '96 – Aucsmith - Huzer et al. as applied above in claims 8-19 and 21 above, further in view of Inoue (U.S. Patent No. 6,011,761)

As per **claim 20**, the combined teachings of Spanos '95 – Schneier '96 – Aucsmith - Huzer et al. discloses a player as applied above in claim 12.

The combined teachings of Spanos '95 – Schneier '96 – Aucsmith - Huzer et al. do not disclose expressly wherein the governed aspect includes use of at least one budget.

Inoue discloses wherein the governed aspect includes use of at least one budget (e.g. abstract, col. 2, lines 11-17, claims 6 and 12).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate the governed aspect includes use of at least one budget into the Spanos '95 – Schneier '96 – Aucsmith - Huzer et al.'s player.

The motivation of doing so would have been to "prevent incorrectly billing the client", as taught by the abstract of Inoue.

### ***Conclusion***

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

Art Unit: 2135

**Contact Information**

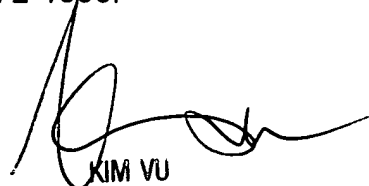
Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS

AYS  
17 January 2007



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100